

A bound on element orders in the holomorph of a finite group

Alexander Bors*

October 8, 2015

Abstract

Let G be a finite group. We prove a theorem implying that the orders of elements of the holomorph $\text{Hol}(G)$ are bounded from above by $|G|$, and we discuss an application to bounding automorphism orders of finite groups.

1 Introduction

1.1 Motivation and main results

Holomorphs are frequently encountered in permutation group theory. For example, it is well-known that a permutation group G acting on a set X and having a regular normal subgroup N is the internal semidirect product of N and the point stabilizer G_x for any $x \in X$, and since the conjugation action of G_x on N is faithful, one obtains a natural embedding $G \hookrightarrow \text{Hol}(N)$. Three of the eight O’Nan-Scott types of finite primitive permutation groups (HA, HS and HC) are of this form.

Conversely, for any group G , $\text{Hol}(G)$ admits a natural faithful permutation representation on (the underlying set of) G in which the canonical copy of G in $\text{Hol}(G)$ is regular; this is by letting $\text{Hol}(G)$ act on G via what the author called *affine maps* in [1, Definition 2.1.1]. In this action, the element $(x, \alpha) \in \text{Hol}(G)$ corresponds to the permutation $A_{x, \alpha} : G \rightarrow G$ sending $g \mapsto x\alpha(g)$. We denote the image of this permutation representation (i.e., the group of bijective affine maps of G) by $\text{Aff}(G)$.

Our motivation for studying holomorphs of finite groups lies in the search for upper bounds on automorphism orders. By [1, Lemma 2.1.4], we have the following: If G is a group, α an automorphism of G , $x \in G$, H an α -invariant subgroup of G

*University of Salzburg, Mathematics Department, Hellbrunner Straße 34, 5020 Salzburg, Austria.
E-mail: alexander.bors@sbg.ac.at

The author is supported by the Austrian Science Fund (FWF): Project F5504-N26, which is a part of the Special Research Program “Quasi-Monte Carlo Methods: Theory and Applications”.

2010 *Mathematics Subject Classification*: 20C25, 20D05, 20D45.

Key words and phrases: Finite groups, Holomorph (group theory), Element orders, Bound.

and gH a coset of H such that $A_{x,\alpha}[gH] \subseteq gH$, say $A_{x,\alpha}(g) = gh_0$ with $h_0 \in H$, then the action of $A_{x,\alpha}$ on gH is isomorphic (in the sense of an isomorphism of finite dynamical systems, see [1, remarks after Definition 1.1.5]) with the action of the bijective affine map $A_{h_0, \alpha|_H}$ on H . Using this, we can prove:

Proposition 1.1.1. *Let G be a finite group, $N \text{ char } G$ and $A = A_{x,\alpha} \in \text{Aff}(G)$. Denote by \tilde{A} the induced affine map on G/N . Then there exists a subset $M \subseteq N$ such that*

$$\text{ord}(A) = \text{ord}(\tilde{A}) \cdot \text{lcm}_{m \in M} \text{ord}(A_{m, (\alpha|_N)^{\text{ord}(\tilde{A})}}).$$

Proof. Clearly, $\text{ord}(\tilde{A}) \mid \text{ord}(A)$, and $A^{\text{ord}(\tilde{A})}$ restricts to a permutation on each coset of N in G . By the remarks before this proposition, for each coset $C \in G/N$, we can fix an element $n_C \in N$ such that the action of $A^{\text{ord}(\tilde{A})}$ on C is isomorphic with the action of $A_{n_C, \alpha|_N^{\text{ord}(\tilde{A})}}$ on N . Set $M := \{n_C \mid C \in G/N\}$. Then clearly, $\text{ord}(A^{\text{ord}(\tilde{A})}) = \text{lcm}_{m \in M} \text{ord}(A_{m, \alpha|_N^{\text{ord}(\tilde{A})}})$, and the result follows. \square

This led the author to studying the following function on finite groups:

Definition 1.1.2. *For a finite group G , define*

$$\mathfrak{F}(G) := \max_{\alpha \in \text{Aut}(G)} \text{lcm}_{x \in G} \text{ord}(A_{x,\alpha}).$$

Clearly, $\mathfrak{F}(G)$ is an upper bound on the maximum element order in $\text{Hol}(G)$, and thus both on the maximum element and maximum automorphism order of G . Our main result is the following upper bound on $\mathfrak{F}(G)$:

Theorem 1.1.3. *For any finite group G , we have $\mathfrak{F}(G) \leq |G|$. In particular, element orders in $\text{Hol}(G)$ are bounded from above by $|G|$.*

It is not difficult to show that $\mathfrak{F}(G) = |G|$ whenever G is a finite cyclic or dihedral group, whence this upper bound is in general best possible. We remark that it is known [6, Theorem 2] that the maximum automorphism order of a nontrivial finite group G is bounded from above by $|G| - 1$. Furthermore, we note that our proof of Theorem 1.1.3 will use the classification of finite simple groups (CFSG). Before tackling the proof, we note an easy consequence. For a finite group G , denote by $\text{mao}(G)$ the maximum automorphism order of G , by $\text{maffo}(G)$ the maximum order of a bijective affine map of G (which coincides with the maximum element order in $\text{Hol}(G)$), and set $\text{mao}_{\text{rel}}(G) := \text{mao}(G)/|G|$ and $\text{maffo}_{\text{rel}}(G) := \text{maffo}(G)/|G|$.

Corollary 1.1.4. *For any finite group G and any characteristic subgroup N of G , we have:*

- (1) $\text{mao}_{\text{rel}}(G/N) \geq \text{mao}_{\text{rel}}(G)$ (mao_{rel} is increasing on characteristic quotients).
- (2) $\text{maffo}_{\text{rel}}(G/N) \geq \text{maffo}_{\text{rel}}(G)$ ($\text{maffo}_{\text{rel}}$ is increasing on characteristic quotients).

Proof. For (1), fix an automorphism α of G such that $\text{ord}(\alpha) = \text{mao}(G)$. In view of Proposition 1.1.1 and Theorem 1.1.3, we deduce that $\text{mao}(G) = \text{ord}(\alpha) \leq \text{ord}(\tilde{\alpha}) \cdot \mathfrak{F}(N) \leq \text{mao}(G/N) \cdot |N|$, and the result follows upon dividing both sides of the inequality by $|G|$. The proof of (2) is analogous. \square

Corollary 1.1.4 extends [3, Lemma 4.3], which dealt with the special case $N = \text{Rad}(G)$, the solvable radical of G .

2 On the proof of Theorem 1.1.3

2.1 Some auxiliary results

In this subsection, we present some results used in the proof of Theorem 1.1.3. We begin by restating [2, Lemma 2.1.6] for the readers' convenience:

Lemma 2.1.1. *Let G be a finite group, $x \in G$, α an automorphism of G . Then every cycle length of $A_{x,\alpha}$ is divisible by $L_G(x, \alpha) := \text{ord}(\text{sh}_\alpha(x)) \cdot \prod_p p^{\nu_p(\text{ord}(\alpha))}$, where p runs through the common prime divisors of $\text{ord}(\text{sh}_\alpha(x))$ and $\text{ord}(\alpha)$. In particular, $L_G(x, \alpha) \mid |G|$. \square*

We can use this to give some sufficient conditions for least common multiples as in the definition of $\mathfrak{F}(G)$ to be bounded by $|G|$:

Lemma 2.1.2. *Let G be a finite group, $\alpha \in \text{Aut}(G)$.*

- (1) *If $\text{ord}(\alpha) \mid |G|$, then $\text{lcm}_{x \in G} \text{ord}(A_{x,\alpha}) \mid |G|$.*
- (2) *For every prime $p \mid |G|$, we have*

$$\text{lcm}_{x \in G} \text{ord}(A_{x,\alpha}) \mid \prod_{q \mid |G|, q \neq p} q^{\nu_q(|G|)} \cdot p^{2\nu_p(\exp(G))} \cdot \exp(\text{Out}(G)).$$

In particular, if, for some prime $p \mid |G|$, we have

$$p^{2\nu_p(\exp(G))} \cdot \exp(\text{Out}(G)) \leq p^{\nu_p(|G|)},$$

then $\text{lcm}_{x \in G} \text{ord}(A_{x,\alpha}) \leq |G|$.

Proof. For (1): Fix $x \in G$. We will show that $\text{ord}(A_{x,\alpha})$, which equals $\text{ord}(\alpha) \cdot \text{ord}(\text{sh}_\alpha(x))$, divides $|G|$. This is tantamount to proving that for any prime p , we have $\nu_p(\text{ord}(\alpha)) + \nu_p(\text{ord}(\text{sh}_\alpha(x))) \leq \nu_p(|G|)$. This is clear (*inter alia* by assumption) if p divides at most one of the two numbers $\text{ord}(\alpha)$ and $\text{ord}(\text{sh}_\alpha(x))$, and if p divides both these numbers, the inequality holds by Lemma 2.1.1.

For (2): Again, we fix $x \in G$. We shall prove that

$$\text{ord}(\alpha) \cdot \text{ord}(\text{sh}_\alpha(x)) \mid \prod_{q \mid |G|, q \neq p} q^{\nu_q(|G|)} \cdot p^{2\nu_p(\exp(G))} \cdot \exp(\text{Out}(G)).$$

Denoting by $\pi : \text{Aut}(G) \rightarrow \text{Out}(G)$ the canonical projection and noting that $\text{ord}(\alpha) = \text{ord}(\pi(\alpha)) \cdot \text{ord}(\alpha^{\text{ord}(\pi(\alpha))})$ with $\text{ord}(\pi(\alpha)) \mid \exp(\text{Out}(G))$, we find that it is sufficient to prove that $\text{ord}(\alpha^{\text{ord}(\pi(\alpha))}) \cdot \text{ord}(\text{sh}_\alpha(x)) \mid \prod_{q \mid |G|, q \neq p} q^{\nu_q(|G|)} \cdot p^{2\nu_p(\exp(G))}$. Fix a prime l . If l divides at most one of the numbers $\text{ord}(\alpha^{\text{ord}(\pi(\alpha))})$ and $\text{ord}(\text{sh}_\alpha(x))$, it is clear that the corresponding inequality of l -adic valuations holds. Hence assume that l divides both these numbers. If $l \neq p$, we are done by an application of Lemma 2.1.1, and if $l = p$, we are done since both orders divide $p^{\nu_p(\exp(G))}$. \square

In view of Lemma 2.1.2, the following well-known technique for bounding the p -exponent of a finite group, particularly of a finite group of Lie type with defining characteristic p , will be useful:

Lemma 2.1.3. *Let p be a prime, K a field of characteristic p , $d \in \mathbb{N}^+$. Let $A \in \mathrm{GL}_d(K)$ be of finite order. Then $\nu_p(\mathrm{ord}(A)) \leq \lceil \log_p(d) \rceil$. In particular, denoting by $d_p(G)$ the minimum faithful projective representation degree in characteristic p of the finite group G , we have $\nu_p(\exp(G)) \leq \lceil \log_p(d_p(G)) \rceil$. \square*

Finally, we note that the function \mathfrak{F} satisfies an inequality which is useful for proofs by induction:

Lemma 2.1.4. *For all finite groups G and $N \mid \mathrm{char} G$, we have $\mathfrak{F}(G) \leq \mathfrak{F}(N) \cdot \mathfrak{F}(G/N)$.*

Proof. Fix an automorphism α of G such that $\mathfrak{F}(G) = \mathrm{lcm}_{x \in G} \mathrm{ord}(A_{x,\alpha}) =: L$. Denote by $\tilde{\alpha}$ the automorphism of G/N induced by α , by $\pi : G \rightarrow G/N$ the canonical projection, and set $L_1 := \mathrm{lcm}_{y \in G/N} \mathrm{ord}(A_{y,\tilde{\alpha}})$. Clearly, $L_1 \leq \mathfrak{F}(G/N)$. On the other hand, setting $L_2 := \mathrm{lcm}_{x \in G} \mathrm{ord}(A_{x,\alpha}^{L_1})$, since each $\mathrm{ord}(A_{x,\alpha})$ divides $L_1 \cdot L_2$, L divides and thus is bounded from above by $L_1 \cdot L_2$, so it suffices to show that $L_2 \leq \mathfrak{F}(N)$. Now as in the proof of Proposition 1.1.1, each $\mathrm{ord}(A_{x,\alpha}^{L_1})$ is a least common multiple of orders of bijective affine maps of N of the form $A_{n,(\alpha|_N)^{L_1}}$ for various $n \in N$. But then L_2 itself is also a least common multiple of such orders, and thus bounded from above by $\mathfrak{F}(N)$, as we wanted to show. \square

2.2 Proof of Theorem 1.1.3

The proof is by induction on $|G|$, with the induction base $|G| = 1$ being trivial. For the induction step, note that if G is not characteristically simple, then fixing any proper nontrivial characteristic subgroup N of G , we have, by Lemma 2.1.4 and the induction hypothesis, $\mathfrak{F}(G) \leq \mathfrak{F}(N) \cdot \mathfrak{F}(G/N) \leq |N| \cdot |G/N| = |G|$. Hence we may assume that G is characteristically simple, i.e., $G = S^n$ for some finite (not necessarily nonabelian) simple group S and $n \in \mathbb{N}^+$.

The case where S is abelian, i.e., $S = \mathbb{Z}/p\mathbb{Z}$ for some prime p , is treated by [3, Lemma 4.3], so we may assume that S is nonabelian. Let us first treat the case $n \geq 2$. Note that by [2, Lemma 3.4] and [6, Theorem 1], we have $\mathrm{mao}(S^n) < |S^n|^{0.438}$. Furthermore, $\exp(S^n) = \exp(S) \leq |S| \leq |S^n|^{0.5}$. It follows that $\mathrm{lcm}_{x \in S^n} \mathrm{ord}(A_{x,\alpha}) = \mathrm{ord}(\alpha) \cdot \mathrm{lcm}_{x \in S^n} \mathrm{ord}(\mathrm{sh}_\alpha(x)) \leq |S^n|^{0.438} \cdot |S^n|^{0.5} < |S^n|$.

We may thus henceforth assume that $G = S$ is a nonabelian finite simple group. It is well-known that the Sylow 2-subgroups of S are not cyclic, whence we are done by Lemma 2.1.2(1) if $\exp(\mathrm{Out}(S)) \leq 2$. This settles all alternating and all sporadic S .

Now assume that S is of Lie type. We will treat this case mostly by applications of Lemma 2.1.2(2), with p always equal to the defining characteristic of S . Hence our goal is to show the inequality $p^{2\nu_p(\exp(S))} \cdot \exp(\mathrm{Out}(S)) \leq p^{\nu_p(|S|)}$, which we do by means of Lemma 2.1.3. Information on $|S|$ and $|\mathrm{Out}(S)|$ is available from [4, p. xvi, Tables 5 and 6], and the values of $d_p(S)$ for the various finite simple groups of Lie type can be found in [7, p. 200, Table 5.4.C].

It is straightforward to verify the sufficient inequality $p^{2\lceil \log_p(d_p(S)) \rceil} \cdot |\text{Out}(S)| \leq p^{\nu_p(|S|)}$ for $S = \text{PSL}_2(p^f)$ with $f \geq 3$, with the exception of the cases $(p, f) = (2, 3), (3, 3), (5, 3)$, for $S = \text{PSL}_d(q)$ with $d \geq 3$, with the exception of $(d, q) = (3, 2), (3, 4)$, and for all S of Lie type which are not isomorphic with any $\text{PSL}_d(q)$.

For $S = \text{PSL}_2(p)$ with $p \geq 5$ or $S = \text{PSL}_2(p^2)$ with $p \geq 3$, we note that $\exp(\text{Out}(S)) = 2$, whence we are done as in the alternating and sporadic case. The same applies to $S = \text{PSL}_3(2)$. Finally, one can check with GAP [5] that for $S = \text{PSL}_2(8), \text{PSL}_2(27), \text{PSL}_2(125), \text{PSL}_3(4)$, all automorphism orders of S divide $|S|$, whence Lemma 2.1.2(1) can be applied to conclude the proof. \square

References

- [1] A. Bors, Classification of finite group automorphisms with a large cycle, to appear in *Comm. Algebra*, arXiv:1410.2284 [math.GR].
- [2] A. Bors, Cycle lengths in finite groups and the size of the solvable radical, preprint (2015), arXiv:1501.07172 [math.GR].
- [3] A. Bors, Finite groups with an automorphism of large order, preprint (2015), arXiv:1509.04607 [math.GR].
- [4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985 (reprinted 2013).
- [5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.5* (2014), <http://www.gap-system.org>.
- [6] M. V. Horoševskiĭ, On automorphisms of finite groups, *Math. USSR-Sb.* **22**(4) (1974), 584–594.
- [7] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series 129, Cambridge University Press, Cambridge, 1990.